Література

1. Блажис, А. К. Дюк, В. А. [Текст] / А. К. Блажис, В. А. Дюк. – СПб.: "СпецЛит". – 2000. – 154 с.
2. Владзимирский, А. В. Модели лучшей практики для телемедицины и электронного здравоохранения [Текст] / А. В. Владзимирский. – Донецк: ООО"Норд". – 2005. – 36 с.
3. Колодій, Р. С. Методи побудови сенсорних мереж мобільного моніторингу ЕКГ [Текст] / Р. С. Колодій, О. В. Тимченко. – НУ ЛП, 2009. – С. 18-22.
4. Гулиев, Я. И. Медицинские информационные системы: теория и практика [Текст] / Я. И. Гулиев, Д. Е. Ермаков, Г. И. Назаренко; ред. Г. И. Назаренко, Г. С. Осипова. – М.: ФИЗМАТЛИТ, 2005. – 320 с.
5. Каплан, Н. Практические основы аналоговых и цифровых схем [Текст] / Н. Каплан, К. Уайт – М.: "Техносфера". – 2006. – 176 с.
6. Heili, B. ZibBee Alliance Tutorial [Electronic resource] . September-November 2005: Proceedings. – Mode of access:www.zigbee.org.
7. Пушкарев, О. И. ZigBee-модули XBee: новые возможности [Текст] / О. Пушкарев // Беспроводные технологии. – 2004. – № 4. – С.22-25.
8. Callaway E. H. Wireless Sensor Networks: Architectures and Photocols [Text] / E. H/ Callaway. – New York: CRC Press LLC, 2004. – 350p.
9. Максимов А. Моделирование устройств на микроконтроллерах с помощью программы ISIS из пакета PROTEUS VSM [Текст] / А. Максимов // Радио. – 2005. – №6. – С. 43-52.
10. Дианов, И. Комплексные решения по GPRS-связи в системах промышленной автоматизации и диспетчеризации [Текст] / И. Дианов, А. Яманов // Беспроводные технологии. –2010. – № 4. – С.32-38.

Визначено правило вибору засобів захисту інформації, що мінімізують значення ризиків на всіх етапах її обробки. Запропонований метод оцінки рівня захищеності інформації на основі аналізу та дослідження динамічних характеристик системи захисту інформації дозволить підвищити ефективність управління захистом інформації із врахуванням змін характеристик процесу захисту

Ключові слова: інформаційні системи, оцінка захищеності, багатокрокові процеси

Определено правило выбора средств защиты информации, которые минимизируют значения рисков на всех этапах её обработки. Предложенный метод оценки уровня защищенности информации на основе анализа и исследования динамических характеристик системы защиты информации позволит повысить эффективность управления защитой информации с учетом изменения характеристик процесса защиты

Ключевые слова: информационные системы, оценка защищенности, многошаговые процессы

УДК 621.391

МЕТОД ОЦІНКИ ЗАХИЩЕНОСТІ ІНФОРМАЦІЇ НА ОСНОВІ БАГАТОКРОКОВИХ ПРОЦЕСІВ ПРИЙНЯТТЯ РІШЕНЬ

А. С. Сторчак
Аспірант
Спеціальна кафедра №4
Інститут спеціально зв'язку та захисту інформації
Національний технічний університет України
«Київський політехнічний інститут»
вул. Московська, 45/1, м. Київ, Україна, 01011
E-mail: storchakanton@gmail.com

1. Вступ

Характер сучасних загроз показує, що загрози розвиваються і модифікуються, кіберзлочинність набуває організованих та цілеспрямованих рис, атаки розгалужені в часі, носять багатокроковий характер, а для їх реалізації використовуються високотехнологічні методи та засоби втручання в роботу інформаційних систем (ІС), збору та обробки даних. Вдосконалення методів та засобів несанкціонованого доступу до ресурсів ІС призводить до розвитку технологій захисту інформації та створенню захищених ІС. Виникає нагальна потреба у вдосконаленні систем захисту інформації (СЗІ).

Серед недоліків сучасних СЗІ є застосування в основному оборонної стратегії захисту від відомих за-

гроз. Тому виникає необхідність ефективного управління як ІС, так й інформаційною безпекою, СЗІ.

Однією із складових систем управління інформаційною безпекою (ІБ) є оцінка рівня захищеності ІС. На відміну від аудиту безпеки, метою якого є визначення ступеня відповідності вимогам стандартів у сфері ІБ, оцінка захищеності ІС призначена для визначення ефективності застосованих засобів захисту (ЗЗ) і формування рекомендацій щодо підвищення безпеки системи [1].

2. Аналіз наукових досліджень

Оцінка стану захищеності ІС повинна проводитися регулярно, на всіх етапах життєвого циклу ІС, при різній мірі повноти і достовірності наявної інформації [2].

На сьогоднішній день вітчизняні та зарубіжні науковці розглядають різні методи та підходи до вирішення задачі оцінки стану захищеності ІС: системний підхід, ймовірнісний підхід, метод експертних оцінок, метод інформаційних потоків, графовий метод, метод вагових коефіцієнтів, підхід, заснований на економічних аспектах, тощо [3 – 9]. Їх основні особливості представлені в [10, 11]. Кожен з пропонованих підходів передбачає розбиття процесу оцінки на декілька етапів, результати яких є невід'ємними складовими процесу оцінки.

3. Мета і постановка задачі

Властивості несанкціонованого впливу на ІС розвиваються з метою реалізації шкідливих дій, а також для ускладнення їх виявлення та протидії. Загрози в загальному випадку є багатоетапними, що вводить залежність форми застосування несанкціонованого впливу від етапів дії на інформацію в ІС.

Одним із завдань СЗІ є оцінка рівня захищеності ІС – необхідно оцінювати стан захищеності ІС в режимі реального часу. Для досягнення цієї мети пропонується досліджувати та аналізувати динамічні характеристики СЗІ на кожному етапі її роботи шляхом використання керованих багатокрокових процесів прийняття рішень. Застосування ЗЗ і отримання оцінки стану захищеності ІС є багатокроковим процесом із n етапами, що характеризуються векторами станів СЗІ X та реалізованих ЗЗ U, і залежить від результатів, що отримано на $n-1$ етапі.

Метою даної роботи є розробка методу оцінки захищеності інформації, що обробляється в ІС на основі керованих багатокрокових процесів прийняття рішень, яка підвищить ефективність управління захистом інформації, враховуючи характеристики процесу захисту.

Для досягнення поставленої мети необхідно визначити значення ризиків R_n на кожному n-ому кроці процесу захисту, а також визначити правило вибору ЗЗ, які мінімізують значення ризиків R на всіх етапах.

Постановка задачі: визначити вектори процесу оцінки стану захищеності $X=\{x_1,...,x_{n-1}\}$ і процесу застосування ЗЗ $U=\{u_1,...,u_{n-1}\}$, що забезпечують мінімізацію значень ризиків R на всіх етапах функціонування СЗІ: $R(U,X)=\min\limits_{U} f(U_n,X_n\,|\,U_{n-1})$.

4. Метод оцінки захищеності інформації

Захищеність інформації залежить від характеристик функціонування СЗІ. Захищеність інформації може змінюватися з часом і є властивістю СЗІ досягати цільового призначення [5]. У динамічних моделях стан захищеності являє собою часовий зріз властивості захищеності інформації і описується значенням відповідного показника в певний фіксований момент часу.

Процес отримання оцінки стану захищеності ІС x і процес застосування ЗЗ u реалізуються по крокам (по етапам) [12]. На кожному n-ому кроці отримується деяка сукупність даних про стан захищеності системи x_n, яка залежить від реалізованих послуг безпеки λ, що характеризують стан захищеності системи і впливають на вибір використовуваних захисних механізмів. Використовуючи отримані і вже відомі відомості про стан захищеності системи $x_n, x_{n-1},...$, приймається рішення u_n про вжиття ЗЗ, яке може залежати і від раніше прийнятих рішень u_{n-1}, u_{n-2}. Якщо $n=1,2,...,N$ то повна сукупність даних про стан захищеності системи x, рішень про ЗЗ u та реалізовані послуги безпеки λ можна описати векторами:

$$x=X_N=\{x_1,...,x_N\};$$

$$u=U_N=\{u_1,...,u_N\};$$

$$\lambda=\Lambda_N=\{\lambda_1,...,\lambda_N\}.$$

Слід врахувати, що задіяні на будь-якому кроці n ЗЗ u_n можуть вплинути на параметри послуг безпеки $\lambda_{n+1},\lambda_{n+2},...$ на наступних кроках, а також на обсяг і якість одержуваних на цих кроках даних про стан захищеності системи $x_{n+1},x_{n+2},...$. Така наявність зворотного зв'язку характерна для систем керування загального вигляду, в яких всі або деякі компоненти рішення u_n є діями, що управляють змінами складу послуг безпеки λ_n та має місце в керованих системах обробки даних. Оскільки будь-які вжиті ЗЗ впливають на значення λ_n і x_n на подальших кроках, а через них на всі наступні ЗЗ, то такі багатокрокові процеси прийняття рішення є керованими [13].

Математичним відображенням цього зворотного зв'язку є залежність розподілів ймовірностей значень λ_n і x_n від послідовності попередньо вжитих ЗЗ $U_{n-1}=\{u_1,...,u_{n-1}\}$.

Повний статистичний опис багатокрокового процесу для будь-якої сукупності прийнятих ЗЗ $u_1,u_2,...$ досягається завданням послідовності умовних розподілів ймовірності (для визначеності щільності ймовірності) для спостережуваних даних і параметрів для всіх значень $n=1,2,...,N$, добуток яких утворює спільну щільність ймовірностей $x=X_N$ і $\lambda=\Lambda_N$ при заданій послідовності ЗЗ $u=U_N$ [13].

При виборі рішень про необхідні ЗЗ u_n можна використовувати тільки ті дані спостереження, які отримані до n-ого кроку включно, тобто $\{x_1,...,x_n\}=X_n$. Тому правило прийняття рішення про застосування

ЗЗ u_n можна задати ймовірнісною мірою з щільністю ймовірностей ϕ_n, яка залежить від X_n, а також від сукупності попередніх рішень $\{u_1,...,u_n\}=U_{n-1}$. У цьому випадку величина ϕ_n буде визначатися виразом:

$$\phi_n=\phi_n(u_n|X_n,U_{n-1}). \quad (1)$$

Знаходження оптимальної послідовності прийняття ЗЗ для багатокрокової процедури проводиться методами динамічного програмування в загальній стохастичній формі [14], які при певних обмеженнях на умови розподілу ймовірності для x_n і λ_n та функцію втрат $g(u,\lambda,x)=g(U_N,\Lambda_N,X_N)$, призводять до ефективної обчислювальної процедури знаходження оптимальних рішень і до аналітичних результатів. При цьому оптимальна послідовність прийняття ЗЗ визначається системою рекурентних співвідношень, яка містить послідовність мінімізацій і усереднень для величин апостеріорних ризиків [13].

Величина середнього ризику визначається виразом:

$$R(\phi)=R(\Phi_N)=M\{g(U_N,\Lambda_N,X_N)\},$$

де $\Phi_N=(\phi_1,\phi_2,...,\phi_N)$ – сукупність щільностей ймовірностей (1), кожна з яких задає правило прийняття ЗЗ на n -ому кроці, а їх добуток – вирішальне правило в цілому.

Нехай оптимальному правилу прийняття рішення про застосування ЗЗ відповідає сукупність Φ_{N0}. Тоді мінімальний (байєсів) середній ризик:

$$R(\Phi_{N0})=\min_{\Phi_N}M\{g(U_N,\Lambda_N,X_N)\}=$$
$$=\min_{\phi_1,...,\phi_{N-1}}\left[\min_{\phi_N}M\{g(U_N,\Lambda_N,X_N)|X_N,U_N\}\right]. \quad (2)$$

Умовне математичне сподівання в (2) являє собою функцію апостеріорного ризику для сукупностей прийнятих ЗЗ U_N і даних про стан системи X_N:

$$R_N(U_N,X_N)=M\{g(U_N,\Lambda_N,X_N)|X_N,U_N\}. \quad (3)$$

Математичне сподівання функції втрат з урахуванням (3) задається виразом:

$$M\{g(U_N,\Lambda_N,X_N)\}=M\{R_N(U_N,X_N)\}=$$
$$=M\left\{\int R_N(U_N,X_N)\phi_N(u_N|X_N,U_{N-1})du_N\right\}.$$

Тоді вираз у квадратних дужках в (2) можна записати у вигляді:

$$\min_{\phi_N}M\{M\{g(U_N,\Lambda_N,X_N)|X_N,U_N\}\}=$$
$$=\min_{\phi_N}M\left\{\int R_N(U_N,X_N)\phi_N(u_N|X_N,U_{N-1})du_N\right\}=$$
$$=M\left\{\min_{\phi_N}\int R_N(U_N,X_N)\phi_N(u_N|X_N,U_{N-1})du_N\right\}=$$
$$=M\left\{\min_{u_N}R_N(U_N,X_N)\right\}.$$

Мінімум виразу $\int R_N(U_N,X_N)\phi_N(u_N|X_N,U_{N-1})du_N$ досягається для функції:

$$\phi_N=\phi_{N0}=\phi_{N0}(u_N|X_N,U_{N-1})=\delta(u_N-u_{N0}(X_N)),$$

де $u_{N0}(X_N)$ – значення u_N, при якому досягається мінімум підінтегрального виразу $R_N(U_N,X_N)$. Це значення визначає оптимальне байєсове правило рішення на N -ому кроці. Воно знаходиться з умови:

$$R_N(u_{N0}(X_N),U_{N-1},X_N)=$$
$$=\min_{u_N}R_N(U_N,X_N)=\tilde{R}_N(U_{N-1},X_N), \quad (4)$$

$$\tilde{R}_N(U_{N-1},X_N)=\min_{u_N}R_N(U_N,X_N)=$$
$$=\min_{u_N}\int g(U_N,\Lambda_N,X_N)p(\Lambda_N|X_N,U_{N-1})d\Lambda_N, \quad (5)$$

є апостеріорний ризик, мінімізований прийнятими ЗЗ u_n на останньому кроці, а $p(\Lambda_N|X_N,U_{N-1})$ – апостеріорна щільність ймовірності сукупності послуг безпеки $\Lambda_N=(\lambda_1,...,\lambda_N)$, яка залежить тільки від стану захищеності ІС на n -ому кроці X_N і від ЗЗ, що приймаються $U_N=(u_1,...,u_{N-1})$.

Апостеріорний ризик на $(N-1)$ кроці знаходиться з повного апостеріорного ризику мінімізацією по u_n і усередненням по x_N:

$$R_{N-1}(U_{N-1},X_{N-1})=M\{\tilde{R}_N(U_{N-1},X_N)|X_{N-1},U_{N-1}\}=$$
$$=\int\tilde{R}_N(U_{N-1},X_N)p_N(\mathbf{x}_N|X_{N-1},U_{N-1})dx_N.$$

Тоді вираз (2) можна записати у вигляді:

$$R(\Phi_{N0})=\min_{\phi_1,...\phi_{N-1}}M\{R_{N-1}(U_{N-1},X_{N-1})\}. \quad (6)$$

Виконавши мінімізацію за останньою з функцій $\phi_1,...,\phi_{N-1}$ представимо (6) наступним чином:

$$R(\Phi_{N0})=\min_{\phi1,...\phi_{N-2}}\left[M\{\tilde{R}_{N-1}(U_{N-2},X_{N-1})\}\right].$$

Оптимальне байєсове правило рішення на $(N-1)$ -ому кроці визначається функцією, яка знаходиться з рівняння $u_{N-1,0}(X_{X-1})$, аналогічно умові (5):

$$R_{R-1}(u_{N-1,0}(X_{X-1}),U_{N-2},X_{N-1}=$$
$$=\min_{u_{N-1}}R_{N-1}(U_{N-1},X_{N-1})=\tilde{R}_{N-1}(U_{N-2},X_{N-1}).$$

Продовжуючи мінімізації для $n=N-2,N-3,...,$ отримаємо співвідношення, яке визначає оптимальне правило вибору ЗЗ на будь-якому кроці:

$$\tilde{R}_n(U_{n-1},X_n)=R_n(u_{n0}(X_n),U_{n-1},X_n)=\min_{u_n}R_n(U_n,X_n). \quad (7)$$

Апостеріорний ризик на n -ому кроці $R_n(U_n,X_n)$ задається співвідношенням, що послідовно визначає функції апостеріорного ризику:

$$R_n(U_n,X_n)=M\left\{\tilde{R}_{n+1}(U_n,X_{n+1})\,|\,X_n,U_n\right\}=$$
$$=M\left\{\min_{u_{n+1}}R_{n+1}(U_{n+1},X_{n+1})\,|\,X_n,U_n\right\}. \quad (8)$$

Спільно з виразами (3) і (4) для кінцевого значення апостеріорного ризику і рівнянням (7) це співвідношення визначає оптимальне багатокрокове правило прийняття ЗЗ.

Разом з виразом (8) можна ввести еквівалентне йому рекурентне співвідношення для апостеріорних ризиків $\tilde{R}_n(U_{n-1},X_n)$, мінімізованих вибором ЗЗ $u_n,u_{n+1},...,u_N$.

Воно отримується з (7) і (8) і має вигляд:

$$\tilde{R}_n(U_{n-1},X_n)=\min_{u_n}\int\tilde{R}_{n+1}(U_n,X_{n+1})p_{n+1}(X_{n+1}\,|\,X_n,U_n)dx_{n+1}. \quad (9)$$

Його відмінністю від (8) є зміна порядку застосування операцій обчислення математичного очікування і мінімізації. Щільність ймовірності $p_{n+1}(X_{n+1}\,|\,X_n,U_n)$, що входить до складу (8) і (9), визначається через щільності $p_n(x_n\,|\,\Lambda_n,X_{n-1},U_{n-1})$ і $p_n(\lambda_n\,|\,\Lambda_n,\Lambda_{n-1},U_{n-1})$ за звичайними правилами теорії ймовірностей.

5. Висновки

Таким чином, рекурентні співвідношення (8) та (9) і правило застосування захисних заходів $u_{n0}(X_n)$ відповідно до (7) визначають процедуру вибору оптимальних заходів із захисту інформації при повному статистичному описі системи. Ці вирази є основою для знаходження оптимальних або близьких до них алгоритмів застосування ЗЗ в разі апріорної невизначеності. Вони дозволяють визначити ступінь захищеності ІС на основі дослідження змін її характеристик.

Запропонований метод полягає в представлені сукупності параметрів СЗІ і синтезі оптимального управління захистом шляхом знаходження оптимальної послідовності реалізації ЗЗ через об'єднану процедуру направленої інтерпретації критерію оптимальності як задачі ідентифікації і наступного її вирішення на умовний екстремум з обмеженнями на параметр керування.

Література

1. Потій, О. В. Дослідження методів оцінки ризиків безпеці інформації та розробка пропозицій з їх вдосконалення на основі системного підходу / О. В. Потій, А. В. Лєншин [Текст] / Збірник наукових праць Харківського університету Повітряних Сил. – 2010. – Вип. 2(24). – С. 85-91.
2. Абрамов, М. А. Стандарты в области информационной безопасности необходимы в управлении организацией [Текст] / М. А. Абрамов // Стандарты и качество. – 2011. – №1. – С. 42-46.
3. Лівенцев, С. П. Огляд моделей безпеки захищених інформаційних систем та використання елементів теорії рефлексивних ігор при їх побудові [Текст]: матеріали науково–практичного семінару / С. П. Лівенцев, А. С. Сторчак / Інформаційні технології у військовій сфері. – Київ, 2012. – Вип. 7. – С. 66-77.
4. Домарев, В. В. Безопасность информационных технологий. Методология создания систем защиты [Текст] / В. В. Домарев. – Изд-во „ДиаСофт", 2002, 688 с.
5. Гарасимчук, О. І. Оцінка ефективності систем захисту інформації [Текст] / О. І. Гарасимчук, Ю. М. Костів / Вісник КНУ ім. Михайла Остроградського. – 2011. – Вип. 1(66), Ч. 1. – С. 16-20.
6. Хнигічева, А. М. Моделювання захищеності складних інформаційно-комунікаційних систем із використанням логіко-ймовірнісного методу [Текст] / А. М. Хнигічева, О. М. Новіков, А. О. Тимошенко / Наукові вісті НТУУ "КПІ". Інформаційні технології, системний аналіз і керування. – 2010. – Вип. 6. – С. 70-77.
7. Грищук, Р. В. Кількісна оцінка рівня захищеності об'єктів електронно-обчислювальної техніки з урахуванням їх функціонування в умовах інформаційного конфлікту [Текст] / Р. В. Грищук // Вісник ЖДТУ Технічні науки: інформатика, обчислювальна техніка. – 2008. – № 3 (46) – С. 113-120.
8. Бурячок, В. Л. Алгоритм оцінювання ступеня захищеності спеціальних інформаційно-телекомунікаційних систем [Текст] / В. Л. Бурячок // Захист інформації. – 2011. – №3. – С. 19-27.
9. Котенко, И. В. Анализ защищенности компьютерных сетей на основе моделирования действий злоумышленников и построения графа атак [Текст] / И. В. Котенко, М. В. Степашкин / Труды ИСА РАН. – 2007. – Т. 31, – С. 126-207.
10. Ливенцев, С. П. Аналіз методів та засобів оцінки захищеності інформаційних систем [Текст]: тези доповідей ВІТІ НТУУ «КПІ» / С. П. Ливенцев, А. С. Сторчак // Науково–практичний семінар «Пріоритетні напрямки розвитку телекомунікаційних систем та мереж спеціального призначення». – 2011. – С. 136.
11. Ливенцев, С. П. Модели и методы анализа защищенности автоматизированных систем [Текст]: тезисы докладов / С. П. Ливенцев, А. С. Сторчак // XV Юбилейная Международная научно-практическая конференция «Безопасность информации в информационно-телекоммуникационных системах». – Киев, 2012. – С. 74-75.
12. Сторчак, А. С. Модель оцінки стану захищеності інформації на основі керованих багатокрокових процесів прийняття рішення [Текст] / А. С. Сторчак // Спеціальні телекомунікаційні системи та захист інформації. – 2013. – №2 (24). – С. 112-117.
13. Репин, В. Г. Статистический синтез при априорной неопределённости и адаптация информационных систем [Текст] / В. Г. Репин, Г. П. Тартаковский. – М.: Советское радио, 1977. – 432 с.
14. Стратонович, Р. Л Условные марковские процессы и их применение к теории оптимального управления [Текст] / Р. Л. Стратонович. – М.: МГУ, 1966, 319 с.